IN THE UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF MISSOURI SOUTHERN DIVISION

IN THE MATTER OF THE SEARCH OF: THE ROOM OCCUPIED BY GABRIEL RAMSEY WITHIN THE RESIDENCE LOCATED AT 1247 EAST SMITH STREET SPRINGFIELD, GREENE COUNTY, MISSOURI 65803	**Case No. 25-SW-2021-DPR**

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Charles Rogener, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this Affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the room occupied by Gabriel Ramsey (the "SUBJECT") within premises known as 1247 East Smith Street, Springfield, Greene County, Missouri 65803 (the "PREMISES"), a location within the Western District of Missouri, as further described in Attachment A, and seizure of items further described in Attachment B.

2. I am a federal law enforcement officer as defined by Rule 41 of the Federal Rules of Criminal Procedure. I am a Special Agent employed by Homeland Security Investigations ("HSI") and have been so employed since February 2019. I am currently assigned to the HSI office in Springfield, Missouri. I am a graduate of the Criminal Investigator Training Program and of the HSI Special Agent Training where I was trained to investigate violations of federal law. I have also received specialized training in computer evidence recovery, and my duties include forensic analysis of electronic devices. I have further received training and gained experience in the use of various surveillance techniques and

the application for and execution of various search, seizure, and arrest warrants, including search warrants of residences and businesses.

3. Prior to becoming a Special Agent, I was employed by Immigration and Customs Enforcement, Enforcement and Removal Operations as a Deportation Officer from July 2006 to February 2019. For two years of my time as a Deportation Officer, I served as a Task Force Officer with the Federal Bureau of Investigation's ("FBI") Safe Streets Task Force, where I was deputized to enforce violations of Titles 18 and 21 of the United States Code. As an FBI Task Force Officer, I participated in several investigations targeting narcotics traffickers and violent gang members. Additionally, I have a Bachelor of Science in Information Technology and a certification in Information System Security from the University of Phoenix.

4. Among other duties, I am currently participating in an investigation relating to allegations of violations of federal laws, including Title 18, United States Code, Section 875(c) (interstate communications containing threat to injure the person of another); and 115(a)(1)(B) (threatening to assault, kidnap, or murder, a federal law enforcement officer).

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, witnesses, and agencies. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. It does not set forth all of my knowledge, or the knowledge of others, about this matter.

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of the Subject Offenses have been committed by the SUBJECT and/or other known or unknown individuals. There is also probable cause

that evidence of the SUBJECT's commission of such crimes is located at the PREMISES. Therefore, there is probable cause to search the PREMISES, further described in Attachment A, for the things described in Attachment B, including for evidence, fruits, and instrumentalities of such criminal violations.

JURISDICTION

7. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined in 18 U.S.C. § 2711. 18 U.S.C. § 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is " a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

APPLICABLE STATUTES

8. Title 18, United States Code, Section 875(c) makes it an offense to transmit in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another.

9. Title 18, United States Code, Section 115(a)(1)(B) makes it an offense to threaten to assault, kidnap, or murder, a federal law enforcement officer.

PROBABLE CAUSE

10. Between January 28 and 30, 2025, Offices of Immigration and Customs Enforcement ("ICE") located in Philadelphia, Pennsylvania; York, Pennsylvania; and San Diego, California received threats from the email address gmramsey@mindspring.com. The emails stated:

> Tom Homan needs to be shot in the head and bleed out real fucking slow so that he has time to think about what a piece of shit he is.

ICE is not about protecting the American people. It is about loudly and visibly removing as many people of color from this country as possible and doing so with great cruelty. It's about sending dumbshit cops with firearms and high school egos into the community to terrorize as many people as possible, to show America who is "really" in charge. For you fascist fucks and your fascist masters, the cruelty is the point.

There are no more rules. If it is accepted for violent right wing fuckjobs like you and your peers to storm the capital to actively interfere with democratic processes, and be rewarded for it, and then to be further resourced to go terrorize the community (particularly vulnerable populations), not just to terrorize them but to cause fear in the rest of the population, as is what is happening now to show that the people need to get in line or they're going to be harmed by the regime, then everyone gets to fight in the same way. There are no more rules, law or norms. That is what your master has told us. "Crime" doesn't matter anymore and all that matters is raw strength. That is how authoritarianism works. That is what your master has said are the rules, and you are now playing by them too. I'll play by those rules as well, just like centuries of resistance to authoritarian rule teaches me. It is not wise to sit back and wait, and say "oh it's just drama" "oh, it will be fine" – no, that's how you wake up in a concentration camp and society falls apart. It took Hitler 5 months to disassemble the Weimar Republic, using the functional system itself.

You are the threat. The threat needs to be eliminated.

ICE are not heroes. They are the enemy. I hope every agent in your field office gets fucking beaten to death with a tire iron. Fucking fascist cunts

Nothing matters anymore. I am going to light myself on fire.

Gabriel M. Ramsey

gmramsey@mindspring.com

415-533-0783

11. On January 30, 2025, the Fresno, California Office of Enforcement and Removal Operations received threats telephonically from telephone number (415) 533-0783. The caller identified himself as the SUBJECT and claimed that he wanted all ICE employees to be shot in the head starting with Tom Homan. The SUBJECT stated that he was calling from a tent and might be outside the Fresno office. The SUBJECT further stated that he wanted to harm himself and others, but that the ICE employee would have to guess in which order he intended to accomplish that.

12. The SUBJECT claimed to have made "hundreds and hundreds" of threats, starting with ICE offices. Specifically, the SUBJECT claimed to have emailed every ICE Office of Principle Legal Counsel. The SUBJECT also claimed to have called United States Secret Service ("USSS") soliciting advice on how to assassinate the President and asking the USSS agents to assassinate the President. Finally, the SUBJECT stated that he was not actively trying to assassinate the President of the United States because, "that Pennsylvania kid" made it too complicated, but if he had a Glock and Donald Trump was right in front of him, he would assassinate the President.

13. On January 30, 2025, agents from Homeland Security Investigations ("HIS") Springfield and officers from the Springfield, Missouri, Police Department knocked at PREMISES, which was believed to be the residence of the SUBJECT's father. A white male adult, later identified as Daniel Ramsey, answered the door and confirmed that the SUBJECT was inside. Mr. Ramsey invited the agents into his home and advised them which room the SUBJECT was located in.

14. In response to a knock on the door, the SUBJECT came out of the room and began yelling about all of the fascists in his father's house. The SUBJECT confirmed calling and emailing ICE offices and reiterated some of the statements made in the emails such as wanting all ICE employees to be shot in the head. The SUBJECT claimed that all ICE employees are "SS" officers and needed to be stopped to avoid slipping into an authoritarian regime. From the context of the conversation, I believe that the SUBJECT was comparing ICE employees to the historical organization, "Schutzstaffel," a paramilitary component of the Nazi party.

15. The SUBJECT stated that he has neither the means nor the intent to act on his threats, but that he has been making threats to ICE employees because he wants them to feel uncertain about their safety whenever they conduct immigration enforcement. When asked if he personally wanted to harm ICE employees, the SUBJECT replied that the agents would just have to guess. The SUBJECT was then handcuffed by the Springfield, Missouri, Police Department officers and transported to the Green County Jail for a phycological evaluation.

16. After the SUBJECT was escorted out of the PREMISES, the SUBJECT's father told the agents that he has been worried about the SUBJECT's mental state. Mr. Ramsey further stated the SUBJECT had spoken of killing himself on several occasions, and that he had settled on accomplishing his own death by either stepping in front of a train or taking a fake gun to the police station. When asked if the SUBJECT had electronic devices, Mr. Ramsey advised the agents that there was a phone and a laptop in the SUBJECT's room. Mr. Ramsey invited the agents to enter the room to see the devices. Upon entering, I observed a laptop and a mobile electronic device on the desk next to the bed. When I picked up the mobile electronic device to place it into airplane mode, I noticed a notepad next the device with, "To Do" written on it. The notes also included a telephone number later identified as the ICE tip line, and the words, "Call Field Offices" as well as a list of cities.

TECHNICAL TERMS

17. Based on my training and experience, and information acquired from other law enforcement officials with technical expertise, I know the terms described below have the following meanings or characteristics:

a. "Digital device," as used herein, includes the following three terms and their respective definitions:

i. A "computer" means an electronic, magnetic, optical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. *See* 18 U.S.C. § 1030(e)(1).

Computers are physical units of equipment that perform information processing using a binary system to represent information. Computers include, but are not limited to, desktop and laptop computers, smartphones, tablets, smartwatches, and binary data processing units used in the operation of other products like automobiles.

ii. "Digital storage media," as used herein, means any information storage device in which information is preserved in binary form and includes electrical, optical, and magnetic digital storage devices. Examples of digital storage media include, but are not limited to, compact disks, digital versatile disks ("DVDs"), USB flash drives, flash memory cards, and internal and external hard drives.

iii. "Computer hardware" means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, modems, routers, scanners, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used

to restrict access to computer hardware (including, but not limited to, physical keys and locks).

b. "Wireless telephone" (or mobile telephone, or cellular telephone), a type of digital device, is a handheld wireless device used for voice and data communication at least in part through radio signals and also often through "wi-fi" networks. When communicating via radio signals, these telephones send signals through networks of transmitters/receivers, enabling communication with other wireless telephones, traditional "land line" telephones, computers, and other digital devices. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of applications and capabilities. These include, variously: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages, email, and other forms of messaging; taking, sending, receiving, and storing still photographs and video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; utilizing global positioning system ("GPS") locating and tracking technology, and accessing and downloading information from the Internet.

c. A "tablet" is a mobile computer, typically larger than a wireless phone yet smaller than a laptop, that is primarily operated by touchscreen. Like wireless phones, tablets function as wireless communication devices and can be used to access the Internet or other wired or wireless devices through cellular networks, "wi-fi"

networks, or otherwise. Tablets typically contain programs called applications ("apps"), which, like programs on both wireless phones, as described above, and personal computers, perform many different functions and save data associated with those functions.

d. A "GPS" navigation device, including certain wireless phones and tablets, uses the Global Positioning System (generally abbreviated "GPS") to display its current location, and often retains records of its historical locations. Some GPS navigation devices can give a user driving or walking directions to another location, and may contain records of the addresses or locations involved in such historical navigation. The GPS consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. "Computer passwords and data security devices" means information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a digital key to "unlock" particular data security devices. Data security hardware

may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

f. "Computer software" means digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

g. Internet Protocol ("IP") Address is a unique numeric address used by digital devices on the Internet. An IP address, for present purposes, looks like a series of four numbers, each in the range 0-255, separated by periods (*e.g.*, 149.101.1.32). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

h. The "Internet" is a global network of computers and other electronic devices that communicate with each other using numerous specified protocols. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

i. "Internet Service Providers," or "ISPs," are entities that provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet, including via telephone-based dial-up and broadband access via digital subscriber line ("DSL"), cable, dedicated circuits, fiber-optic, or satellite. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name, a username or screen name, an email address, an email mailbox, and a personal password selected by the subscriber. By using a modem, the subscriber can establish communication with an ISP and access the Internet by using his or her account name and password.

j. A "modem" translates signals for physical transmission to and from the ISP, which then sends and receives the information to and from other computers connected to the Internet.

k. A "router" often serves as a wireless Internet access point for a single or multiple devices, and directs traffic between computers connected to a network (whether by wire or wirelessly). A router connected to the Internet collects traffic bound for the Internet from its client machines and sends out requests on their behalf. The router also distributes to the relevant client inbound traffic arriving from the Internet. A router usually retains logs for any devices using that router for Internet connectivity. Routers, in turn, are typically connected to a modem.

l. "VPN" means a virtual private network. A VPN extends a private network across public networks like the Internet. It enables a host computer to send and receive data across shared or public networks as if they were an integral part of a private network with all the functionality, security, and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two. The VPN connection across the Internet is technically a wide area network ("WAN") link between the sites. From a user perspective, the extended network resources are accessed in the same way as resources available from a private network-hence the name "virtual private network." The communication between two VPN endpoints is encrypted and usually cannot be intercepted by law enforcement.

m. "Encryption" is the process of encoding messages or information in such a way that eavesdroppers or hackers cannot read it, but authorized parties can. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, turning it into an unreadable ciphertext. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any unintended party that can see the ciphertext should not be able to determine anything about the original message. An authorized party, however, is able to decode the ciphertext using a decryption algorithm that usually requires a secret decryption key, to which adversaries do not have access.

COMPUTERS, ELECTRONIC/MAGNETIC STORAGE, AND FORENSIC ANALYSIS

18. As described above and in Attachment B, this application seeks permission to search for

evidence, fruits, contraband, instrumentalities, and information of the aforementioned offenses that might be found on the PREMISES, in whatever form they are found. One form in which such items might be found is data stored on one or more digital devices. Such devices are defined above and include any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop computers, laptop computers, notebooks, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, USB flash drives, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Thus, the warrant applied for would authorize the seizure of digital devices or, potentially, the copying of stored information, all under Rule 41(e)(2)(B). Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit that, if digital devices are found on the PREMISES, there is probable cause to believe that the items described in Attachment B will be stored in the device(s) for at least the following reasons:

a. Individuals who engage in criminal activity, including 18 U.S.C. §§ 875(c) (interstate communications containing threat to injure the person of another), use digital devices, to access websites to facilitate illegal activity and to communicate

threats online or through a phone conversation; to store on digital devices, documents and records relating to their illegal activity, which can include logs of online chats; email correspondence; text or other "Short Message Service" ("SMS") messages; the Subjects have/or have had email accounts and cellular or other telephones which were used to communicate specific threats furthering their criminal activity.

b. Individuals who engage in the foregoing criminal activity, in the event that they change digital devices, will often "back up" or transfer files from their old digital devices to that of their new digital devices, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity.

c. Digital device files, or remnants of such files, can be recovered months or even many years after they have been downloaded onto the medium or device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensics tools. When a person "deletes" a file on a digital device such as a home computer, a smart phone, or a memory card, the data contained in the file does not actually disappear; rather, that data remains on the storage medium and within the device unless and until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the digital device that is not allocated to an active file or that is unused after a file has been allocated

to a set block of storage space – for long periods of time before they are overwritten. In addition, a digital device's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of electronic storage medium space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve "residue" of an electronic file from a digital device depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer, smart phone, or other digital device habits.

19. As further described in Attachment B, this application seeks permission to locate not only electronic evidence or information that might serve as direct evidence of the crimes described in this affidavit, but also for forensic electronic evidence or information that establishes how the digital device(s) were used, the purpose of their use, who used them (or did not), and when. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit there is probable cause to believe that this forensic electronic evidence and information will be in any of the devices located at the PREMISES because:

a. Although some of the records called for by this warrant might be found in the form of user-generated documents or records (such as word processing, picture, movie, or texting files), digital devices can contain other forms of electronic evidence as

well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials contained on the digital device(s) are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive, flash drive, memory card, or other electronic storage media image as a whole. Digital data stored in the Device(s), not currently associated with any file, can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on a hard drive that show what tasks and processes on a digital device were recently used. Web browsers, email programs, and chat programs often store configuration data on a hard drive, flash drive, memory card, or memory chip that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times a computer, smart phone, or other digital device was in use. Computer, smart phone, and other digital device file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

b. Forensic evidence on a digital device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, chats, instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time, and potentially who did not.

c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how such digital devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, digital device evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on digital devices is evidence may depend on other information stored on the devices and the application of knowledge about how the devices behave. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular

thing is not present on the device. For example, the presence or absence of counter-forensic programs, anti-virus programs (and associated data), and malware may be relevant to establishing the user's intent and the identity of the user.

METHODS TO BE USED TO SEARCH DIGITAL DEVICES

20. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I know that:

a. Searching digital devices can be an extremely technical process, often requiring specific expertise, specialized equipment, and substantial amounts of time, in part because there are so many types of digital devices and software programs in use today. Digital devices – whether, for example, desktop computers, mobile devices, or portable storage devices – may be customized with a vast array of software applications, each generating a particular form of information or records and each often requiring unique forensic tools, techniques, and expertise. As a result, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched, and to obtain specialized hardware and software solutions to meet the needs of a particular forensic analysis.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. Recovery of

"residue" of electronic files from digital devices also requires specialized tools and often substantial time. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is often essential to conducting a complete and accurate analysis of data stored on digital devices.

c. Further, as discussed above, evidence of how a digital device has been used, the purposes for which it has been used, and who has used it, may be reflected in the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data or software on a digital device is not segregable from the digital device itself. Analysis of the digital device as a whole to demonstrate the absence of particular data or software requires specialized tools and a controlled laboratory environment, and can require substantial time.

d. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear as though the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form.

Digital device users may encode communications or files, including substituting innocuous terms for incriminating terms or deliberately misspelling words, thereby thwarting "keyword" search techniques and necessitating continuous modification of keyword terms. Moreover, certain file formats, like portable document format ("PDF"), do not always lend themselves to keyword searches. Some applications for computers, smart phones, and other digital devices, do not store data as searchable text; rather, the data is saved in a proprietary non-text format. Documents printed by a computer, even if the document was never saved to the hard drive, are recoverable by forensic examiners but not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography, a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband, or instrumentalities of a crime.

e. Analyzing the contents of mobile devices, including tablets, can be very labor intensive and also requires special technical skills, equipment, and software. The large, and ever increasing, number and variety of available mobile device applications generate unique forms of data, in different formats, and user

information, all of which present formidable and sometimes novel forensic challenges to investigators that cannot be anticipated before examination of the device. Additionally, most smart phones and other mobile devices require passwords for access. For example, even older iPhone 4 models, running iOS 7, deployed a type of sophisticated encryption known as "AES-256 encryption" to secure and encrypt the operating system and application data, which could only be bypassed with a numeric passcode. Newer cell phones employ equally sophisticated encryption along with alpha-numeric passcodes, rendering most smart phones inaccessible without highly sophisticated forensic tools and techniques, or assistance from the phone manufacturer. Mobile devices used by individuals engaged in criminal activity are often further protected and encrypted by one or more third party applications, of which there are many. For example, one such mobile application, "Hide It Pro," disguises itself as an audio application, allows users to hide pictures and documents, and offers the same sophisticated AES-256 encryption for all data stored within the database in the mobile device.

f. Based on all of the foregoing, I respectfully submit that searching any digital device for the information, records, or evidence pursuant to this warrant may require a wide array of electronic data analysis techniques and may take weeks or months to complete. Any pre-defined search protocol would only inevitably result in over- or under-inclusive searches, and misdirected time and effort, as forensic examiners encounter technological and user-created challenges, content, and software applications that cannot be anticipated in advance of the forensic

examination of the devices. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques reasonably appear to be necessary to locate and retrieve digital information, records, or evidence within the scope of this warrant.

21. The volume of data stored on many digital devices will typically be so large that it will be extremely impractical to search for data during the physical search of the premises.

a. Therefore, in searching for information, records, or evidence, further described in Attachment B, law enforcement personnel executing this search warrant will employ the following procedures:

1. Upon securing the PREMISES, law enforcement personnel will, consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, seize any digital devices (that is, the Device(s)), within the scope of this warrant as defined above, deemed capable of containing the information, records, or evidence described in Attachment B and transport these items to an appropriate law enforcement laboratory or similar facility for review. For all the reasons described above, it would not be feasible to conduct a complete, safe, and appropriate search of any such digital devices at the PREMISES. The digital devices, and/or any digital images thereof created by law enforcement sometimes with the aid of a technical expert, in an appropriate setting, in aid of the examination and review, will be examined and reviewed in order to extract and seize the information, records, or evidence described in Attachment B.

2. The analysis of the contents of the digital devices may entail any or all of various forensic techniques as circumstances warrant. Such techniques may include, but shall not be limited to, surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); conducting a file-by-file review by "opening," reviewing, or reading the images or first few "pages" of such files in order to determine their precise contents; "scanning" storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic "keyword" searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

3. In searching the digital devices, the forensic examiners may examine as much of the contents of the digital devices as deemed necessary to make a determination as to whether the contents fall within the items to be seized as set forth in Attachment B. In addition, the forensic examiners may search for and attempt to recover "deleted," "hidden," or encrypted data to determine whether the contents fall within the items to be seized as described in Attachment B. Any search techniques or protocols used in searching the contents of the seized digital devices will be specifically chosen to identify the specific items to be seized under this warrant.

CONCLUSION

22. Based upon the evidence set forth herein, there is probable cause to search the PREMISES, fully described in Attachment A, for the items listed in Attachment B, which are evidence of, property used in, and contraband and fruits of, the commission of crimes, specifically violations of 18 U.S.C. §§ 875(c) (interstate communications containing threat to injure the person of another); and 115(a)(1)(B) (threaten to assault or murder a federal law enforcement officer).

23. The facts set forth in this affidavit are true and correct to the best of my knowledge and belief. Wherefore, I request the issuance of the requested warrant.

Further Affiant Sayeth Naught.

Charles Rogener
Special Agent
Homeland Security Investigations

Sworn to and subscribed to before me in my presence via telephone on this 30th day of January 2025.

The Honorable Willie J. Epps, Jr.
Chief United States Magistrate Judge
Western District of Missouri